Economic implications of the Investigatory Powers Bill

techUK briefing note for Shadow Treasury Team

In March 2016, the Home Office published a revised Investigatory Powers Bill and the Government's response to pre-legislative scrutiny. techUK members take their legal responsibilities to work with the security services extremely seriously.

In light of recent events and the current climate of global security concerns, it is even more important that a clear legal framework for investigatory powers is established; **one that is worthy of emulation around the world and is a cornerstone of an international framework that is transparent, workable and predictable for global companies, agencies and citizens.** techUK has a number of concerns with the revised Bill as it progresses through both Houses, and this briefing note outlines a number significant economic implications arising from the current wording of the Bill. Note that techUK has also been in parallel discussions with the shadow Home Office team.

Context

Britain's digital economy is the largest in Europe, accounting for nearly 15 per cent of GDP and more than 1.5 million jobs. Recent governments have championed the growth of digital business by supporting Tech City and incentives for entrepreneurs to start new ventures. Companies and users of digital services have a shared interest in the sector's continued growth.

As outlined in a recent letter from tech leaders published in the Telegraph, the success of the UK's digital economy fundamentally depends on the trust of customers and users. Our members take significant steps to earn and safeguard this trust, in part achieved by ensuring that there are appropriate legal frameworks in place to protect users' data. A crucial element of user trust is ensuring that there is a robust and transparent process in place whereby companies can honour lawful requests for data by government authorities. These must be set out in clear and predictable laws.

Whilst techUK appreciates the Government's commitment to bringing legislation in this area within a single Investigatory Powers Bill, **there is growing anxiety among businesses about the potential ramifications of the powers in the Bill for user confidence in digital services**. For example, attempting to enforce UK laws on foreign companies could lead other governments to do the same, to the detriment of UK businesses. This is a serious matter and we believe it is critically important that sufficient scrutiny is given to economic implications of the Bill.

We encourage the Government to look at a bigger picture and longer time horizon in terms of the impact the Bill could have on the UK's economy, particularly in light of the forthcoming UK Digital Strategy to be published by Government. Digital companies require clarity and consistency and the Bill falls short of achieving that end on a number of fronts.

techUK

Issue 1 – The Bill threatens to undermine the foundations of trust of the UK's Digital Economy

Since 2010 there has been growing public concern into how surveillance is conducted in the UK, with recent surveys revealing that 72% of British consumers are concerned about their private information online.[1] Small shifts in public sentiment regarding the security and privacy of users' communications can have serious consequences for the UK's digital economy. This is why many companies publish transparency reports for consumers – ensuring that citizens are fully informed of issues related to surveillance and privacy.

Whilst many of the provisions within the Investigatory Powers Bill are vague and broad in their scope, the safeguards afforded to these provisions are limited in nature. This creates highly problematic legal uncertainty for companies and undermines trust in the UK's digital economy and confidence in the UK as a place to do data-driven business.

For example, the Bill provides a framework for the security services to "interfere" with any equipment that produces "electromagnetic, acoustic or other emissions". However, alongside this broad power, companies are required to "take all steps to give effect" to such a warrant without being able to notify anyone. This lack of transparency with such a broad power will only limit the trust of consumers with products and services provided for in the UK.

Issue 2 – The Bill raises serious question marks for rapidly growing tech companies

Technology companies are constantly innovating and developing their services and products in order to rapidly grow. The uncertainty within the Bill will therefore have a significant impact on the growth of small and medium sized enterprises (SMEs), many of whom are unaware of the new requirements within the Bill that may affect them.

For example, the Bill can impose an obligation on a small cloud provider to retain data after the data controller, i.e. the customer in some cases, has deleted the data. This will make the small provider the de-facto data controller and create a host of obligations that differ from the normal practice of cloud providers, where responsibility for data is shared between the hosting provider and customer.

A number of start-ups have thus already decided to leave the UK due to the far reaching nature of the legislation and the requirements to diverge from normal business practices through retaining certain types of data.

Issue 3 – Economic security and national security are two sides of the same coin

The resiliency of a company's security is a fundamental aspect of their ability to compete in a global market. Technology companies have several legal obligations, from the Data Protection Act to the upcoming Network and Information Security Directive, to ensure the security of their networks, services and customers' data. Although the Government stresses that it wants to improve

[1] The research, conducted by YouGov, surveyed more than 2,000 British adults

UK cyber security, the Bill is unclear on whether the government will allow companies to use end to end encryption to protect themselves and their customers.

Encryption is fundamental for UK GDP and underpins the fabric behind the digital economy. It is widely seen as the best method to ensure that businesses and government are not vulnerable to online attacks and fulfil their legal obligations under data protection statutes to keep personal data free from external intrusion. Such ambiguity around encryption will not only weaken the security of the digital economy, but also reduce the desire of companies to develop products in such an unsecure business environment.

Issue 4 – The Bill is unclear on the implications of data retention costs for the exchequer

The Bill is highly ambiguous on the cost implications of certain measures on companies. Though the cost implications of the proposals in the Bill will differ between companies based on size, date of entrance into the market and current capabilities, requiring the retention of ICRs is a significant change for internet service providers and will add additional operational costs due to the vast amounts of data that passes through the internet on a daily basis. Despite this, the Bill only makes provision for "an appropriate contribution…that must never be nil" towards costs of retaining data that companies would not normally retain for business purposes.

The issue of costs is important, since it introduces an element of proportionality as to why a certain provision is required. If Government is made responsible for meeting the full costs, this would provide an important check to ensure that the powers the Government seek to implement are proportionate.

Issue 5 – Potential conflicts of the Bill

Communication services are increasingly being provided on a global basis. The extra-territorial assertions in the Bill, when considered alongside the recently agreed General Data Protection Regulation, NIS Directive and other statutes which require companies to keep data secure, will result in a patchwork of overlapping and conflicting laws that creates uncertainty, undermines user privacy and hinders innovation.

This will make the UK a harder place to do business and is a disincentive to investment and innovation. It also sets a worrying international precedent: UK companies abroad might find themselves having to retain and provide data to satisfy overseas governments.

Issue 6 – Encouraging joined up Government

techUK encourages HM Treasury and the Department of Business, Innovation and Skills rigorously examine the economic impacts of the Bill based on the above concerns. It is unclear whether the full economic implications of the Bill have been fully considered with industry. In light of the Government's forthcoming UK Digital Strategy which seeks to position the UK as a global leader, such an assessment is crucial for the UK's ongoing economic priorities.

About techUK

techUK represents the companies and technologies that are defining today the world that we will live in tomorrow. More than 850 companies are members of techUK. Collectively they employ approximately 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium sized businesses.

Contact

Talal Rajab
Head of Programme – Cyber and National Security
talal.rajab@techuk.org
020 7331 2189

Charlotte Holloway
Head of Policy / Associate Director
charlotte.holloway@techuk.org
+ 44 (0) 7710 320795